UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,696	09/12/2003	David D. Brandt	03AB014C/ALBRP303USC	7375

7590 06/21/2007

Susan M. Donahue
Rockwell Automation, 704-P, IP Department
1201 South 2nd Street
Milwaukee, WI 53204

EXAMINER	
BAUM, RONALD	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
06/21/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/661,696	BRANDT ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 April 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-41* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-41* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *12 September 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *20070614*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in reply to applicant's correspondence of 19 April 2007.

2. Claims 1-41 are pending for examination.

3. Claims 1-41 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-41 are rejected under 35 U.S.C. 102(b) as being anticipated by Swiler et al, U.S. Patent 7,013,395 B1.

5. As per claim 1; "A security analysis tool for an automation system, comprising:

an interface component to generate

a description of factory assets [ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a

function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]; and

an analyzer component to generate

one or more security outputs

based on the description [ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.].".

As per claim 12, this claim is the method claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A security analysis method, comprising:

inputting a at least

one model related to

one or more factory assets; and

generating

one or more security outputs

based on the model.".

As per claim 16, this claim is the means plus function claim for the system claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; "A security analysis system in an automation environment, comprising:

means for receiving abstract descriptions

of at least one of

factory assets and

network devices; and

means for generating

one or more security outputs

based on the abstract description; and

means for automatically distributing

the security outputs

to facilitate network security in the automation environment.".

6. Claim 2 ***additionally recites*** the limitation that; "The tool of claim 1,

at least one of

the interface component and

the analyzer component

operate on a computer and

receive

one or more factory inputs

that provide the description.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

7. Claim 3 ***additionally recites*** the limitation that; "The tool of claim 2,

the factory inputs include

user input,

model inputs,

schemas,

formulas,

equations,

files,

maps, and

codes.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system

analysis tool using inputted (i.e., interface component utilizing, at the very least, user input, model inputs, files, maps, and codes) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

8. Claim 4 ***additionally recites*** the limitation that; "The tool of claim 2,

the factory inputs are processed by

the analyzer component to generate the security outputs,

the security outputs including

at least one of

manuals,

documents,

schemas,

executables,

codes,

files,

e-mails,

recommendations,

topologies,

configurations,

application procedures,

parameters,

policies,

rules,

user procedures, and

user practices

that are employed

to facilitate security measures in

an automation system.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

9. Claim 5 ***additionally recites*** the limitation that; "The tool of claim 1,

the interface component includes

at least one of

a display output having associated display objects and

at least one input

to facilitate operations with

the analyzer component,

the interface component is associated with

at least one of

an engine,

an application,

an editor tool,

a web browser, and

a web service.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

10. Claim 6 ***additionally recites*** the limitation that; "The tool of claim 5,

the display objects include

at least one of

configurable icons,

buttons,

sliders,

input boxes,

selection options,

menus, and

tabs,

the display objects having

multiple configurable

dimensions,

shapes,

colors,

text,

data and

sounds

to facilitate operations with

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system

analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

11. Claim 7 ***additionally recites*** the limitation that; "The tool of claim 5,

the at least one inputs includes

receiving user commands from

a mouse,

keyboard,

speech input,

web site,

remote web service,

camera, and

video input

to affect operations of

the interface component and

the analyzer component.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted (i.e., interface component, utilizing, at the very least, GUI oriented input editing tools, and a display output having associated display objects for the results graphic output) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

12. Claim 8 ***additionally recites*** the limitation that; "The tool of claim 1,

the description includes

a model of one or more automation assets

to be protected and

associated network pathways

to access the automation assets.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes

recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

13. Claim 9 ***additionally recites*** the limitation that; "The tool of claim 1,

the description

includes at least one of

risk data and

cost data

that is employed by

the analyzer component

to determine suitable security measures.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model, clearly dealing with risk and effective cost insofar as network security per se is concerned) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 13, this claim is the method claim for the system claim 9 above, and is rejected for the same reasons provided for the claim 9 rejection; "The method of claim 12,

the at least one model is related to

at least one of

a risk-based model and

a cost-based model.".

14. Claim 10 ***additionally recites*** the limitation that; "The tool of claim 1,

the description

includes at least one of

shop floor access patterns,

Intranet access patterns,

Internet access patterns, and

wireless access patterns.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., description of factory assets, clearly dealing with Intranet and Internet access patterns insofar as network security per se is concerned) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the

changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

15. Claim 11 ***additionally recites*** the limitation that; "The tool of claim 1,

the analyzer component is adapted for

partitioned security specification entry and

sign-off from various groups.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., the network partitioned security specification) and attack template (i.e., inclusive of authentication aspects, insofar as sign-on/sign-off, at the very least would be concerned) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

16. Claim 14 ***additionally recites*** the limitation that; "The method of claim 12,

the security outputs include at least one of recommended

security components,

codes,

parameters,

settings,

related interconnection topologies,

connection configurations,

application procedures,

security policies,

rules,

user procedures, and

user practices.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, recommendations, files, rules, configurations)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

17. Claim 15 ***additionally recites*** the limitation that; "The method of claim 12, further comprising at least one of:

automatically deploying the security outputs

to one or more entities; and

utilizing the security outputs

to mitigate at least one of

unwanted network access and

network attack.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

18. As per claim 17; "A security validation system, comprising:

a scanner component

to automatically interrogate an automation system

at periodic intervals for

security related data [ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system

structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.]; and

a validation component

to automatically assess security capabilities of the automation system

based upon a comparison of

the security related data and

one or more predetermined security guidelines [ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (i.e., a validation component ...) as a function of the risks and costs associated with the changes recommended, clearly

encompassing the claimed limitations as broadly interpreted by the examiner.].".

As per claim 26, this claim is the method claim for the system claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection; "An automated security validation method, comprising:

scanning one or more networks or automation devices for

potential security violations; and

performing an automated security procedure if

a security violation is detected.".

As per claim 30, this claim is the means plus function claim for the system claim 17 above, and is rejected for the same reasons provided for the claim 17 rejection; "An automated security validation system, comprising:

means for scanning one or more networks or automation devices for

potential security violations;

means for initiating a security procedure in response to

the security violations; and

means for performing at least one of

security assessments,

security compliance checks; and

security vulnerability scanning

to mitigate the security violations.".

19. Claim 18 ***additionally recites*** the limitation that; "The system of claim 17,

the scanner component and

the validation component

are at least one of

a host-based component and

a network-based component.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., scanner component) computer system/network configuration/topology (i.e., description of factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

20. Claim 19 ***additionally recites*** the limitation that; "The system of claim 17,

the validation component performs at least one of

a security audit,

a vulnerability scan,

a revision check,

an improper configuration check,

file system check,

a registry check,

a database permissions check,

a user privileges check,

a password check, and

an account policy check.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component, insofar as associated with improper configuration, vulnerability, file system check, user privileges check, etc.,), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

21. Claim 20 ***additionally recites*** the limitation that; "The system of claim 17,

the security guidelines

are automatically determined.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

22. Claim 21 ***additionally recites*** the limitation that; "The system of claim 18,

the host-based component performs

vulnerability scanning and

auditing on devices,

the network-based component performs

vulnerability scanning and

auditing on networks.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes

recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

23. Claim 22 ***additionally recites*** the limitation that; "The system of claim 21,

at least one of

host-based component and

the network-based component

at least one of

determines susceptibility to

common network-based attacks,

searches for

open TCP/UDP ports,

scans for

vulnerable network services,

attempts to gain identity information about

end devices that relates to

hacker entry,

performs vulnerability

scanning and

auditing

on

firewalls,

routers,

security devices, and

factory protocols.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

As per claim 27, this claim is the method claim for the system claim 22 above, and is rejected for the same reasons provided for the claim 22 rejection; "The method of claim 26, further comprising at least one of:

checking for

susceptibility to network-based attacks;

searching for

open TCP/UDP ports; and

scanning for

vulnerable network services.".

24. Claim 23 ***additionally recites*** the limitation that; "The system of claim 21,

at least one of

host-based component and

the network-based component

at least one of

includes

non-destructively mapping a topology of

IT and

automation devices,

checking revisions and configurations,

checking user attributes, and

checking access control lists.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based/network-based component) analysis tool using inputted (i.e., vulnerability scanner component) computer system/network configuration/topology (i.e., auditing factory assets) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

25. Claim 24 ***additionally recites*** the limitation that; "The system of claim 17, further comprising

a component to automatically initiate a security action

in response to

detected security problems.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., automatically initiate a security action), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

26. Claim 25 ***additionally recites*** the limitation that; "The system of claim 24,

the security action includes at least one of

automatically correcting security problems,

automatically adjusting security parameters,

altering network traffic patterns,

add security components,

removing security components,

firing alarms,

automatically notifying entities about detected problems and concerns,

generating an error or log file,

generating a schema,

generating data to re-configure or re-route network connections,

updating a database, and

updating a remote site.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information, such that results (i.e., post analysis generated security outputs) used to evaluate (i.e., graphed output information, utilizing, at the very least, topologies, automatically notifying entities about detected problems and concerns, generating an error or log file, generating data to re-configure or re-route network connections, updating a database, etc.,)/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

27. Claim 28 ***additionally recites*** the limitation that; "The method of claim 26, further comprising at least one of:

automatically performing security assessments;

automatically performing security compliance checks; and

automatically performing security vulnerability scanning.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., automatically performing security assessments, etc.,), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

28. Claim 29 ***additionally recites*** the limitation that; "The method of claim 26, the automated security procedures include at least one of

automatically performing corrective actions,

altering network patterns,

adding security components,

removing security components,

adjusting security parameters, and

generating security data to mitigate network security problems.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to

evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., adjusting security parameters, generating security data to mitigate network security problems, etc.,), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

29. As per claim 31; "A security learning system for an automation environment, comprising:

a learning component

to monitor and learn automation activities during

a training period [ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.];

and

a detection component

to automatically trigger a security event based upon

detected deviations of subsequent automation activities

after the training period [ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (i.e., a detection component ... trigger a security event ... after the training period) as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.].".

As per claim 39, this claim is the method claim for the system claim 31 above, and is rejected for the same reasons provided for the claim 31 rejection; "A security learning method, comprising:

monitoring a network for

a predetermined time;

automatically learning

at least one data pattern during

the predetermined time; and

generating an alarm if

a current data pattern is determined to be

outside of a predetermined threshold associated with

the at least one data pattern.".

As per claim 41, this claim is the means plus function claim for the system claim 31 above, and is rejected for the same reasons provided for the claim 31 rejection; "A security learning system in an automation environment, comprising:

means for

scanning a network;

means for

learning data patterns from the network; and

means for

generating a security event if

current data patterns are determined to be

out of tolerance from stored data patterns.".

30. Claim 32 ***additionally recites*** the limitation that; "The system of claim 31, the automation activities includes at least one of

a network activity and

a device activity.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system (i.e., host-based device activity /network-based activity component) analysis tool using inputted (i.e., scanner automation activities component) computer system/network configuration/topology and attack template information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended (i.e., validation component), clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

31. Claim 33 ***additionally recites*** the limitation that; "The system of claim 31,

the learning component including

at least one of

a learning model and

a variable.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results

used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

32. Claim 34 ***additionally recites*** the limitation that; "The system of claim 31,

the automation activities include

at least one of

a number of network requests,

a type of network requests,

a time of requests,

a location of requests,

status information, and

counter data.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities, such as number of network requests, type of network requests, location of requests, etc.,) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a

function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

33. Claim 35 ***additionally recites*** the limitation that; "The system of claim 31,

the detection component employs

at least one of

a threshold and

a range to determine the deviations.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning detection/monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities, such as number of network requests, type of network requests, location of requests, etc.,) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

34. Claim 36 ***additionally recites*** the limitation that; "The system of claim 35,

the threshold and

the range

are dynamically adjustable.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning detection/monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities, such as number of network requests, type of network requests, location of requests, etc.,) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

35. Claim 37 ***additionally recites*** the limitation that; "The system of claim 33,

the learning model includes

at least one of

mathematical models,

statistical models,

probabilistic models,

functions,

algorithms, and

neural networks,

classifiers,

inference models,

Hidden Markov Models (HMM),

Bayesian models,

Support Vector Machines (SVM),

vector-based models, and

decision trees.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized (i.e., mathematical, statistical, probabilistic models, etc.,) attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

36. Claim 38 ***additionally recites*** the limitation that; "The system of claim 31,

the security event includes

at least one of

automatically performing corrective actions,

altering network patterns,

adding security components,

removing security components,

adjusting security parameters,

firing an alarm, notifying an entity,

generating an e-mail,

interacting with a web site, and

generating security data

to mitigate network security problems.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., model) information dealing with hypothesized attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities (i.e., security event ... altering network patterns ... adjusting security parameters, generating security data, etc.,) as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

37. Claim 40 ***additionally recites*** the limitation that; "The method of claim 39,

the at least one data pattern

employed as input for

a security analysis process.".

The teachings of Swiler et al are directed towards such limitations (i.e., ABSTRACT, figures 1-2 and associated descriptions, col. 3,lines 10-col. 9,line 19, whereas the provided computer system analysis tool (i.e., learning/ monitoring/scanning component) using inputted computer system/network configuration/topology (i.e., polling/automatically interrogating of network machines (periodic interval scanning of automation activities) and gathering associated data such as IP address, machine type, operating system, file system structure, etc.,) and attack template (i.e., learning model) information dealing with hypothesized (i.e., mathematical, statistical, probabilistic models, etc.,) attack scenario(s), such that results used to evaluate/make configuration changes in the network to counter vulnerabilities as a function of the risks and costs associated with the changes recommended, clearly encompassing the claimed limitations as broadly interpreted by the examiner.).

Conclusion

38. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861 and unofficial email is Ronald.baum@uspto.gov. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at (571) 272-4195. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

6/19/07